**Приказ ФСБ РФ от 27 декабря 2011 г. № 796**
**«Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»**

В соответствии с **частью 5 статьи 8** Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»* приказываю:

Утвердить:

- Требования к средствам электронной подписи (**приложение № 1**);
- Требования к средствам удостоверяющего центра (**приложение № 2**).

Директор А. Бортников

---

* Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880.

Зарегистрировано в Минюсте РФ 9 февраля 2012 г.
Регистрационный № 23191

**Приложение № 1**
**к приказу ФСБ РФ**
**от 27 декабря 2011 г. № 796**

# Требования к средствам электронной подписи

## I. Общие положения

1. Настоящие Требования разработаны в соответствии с **Федеральным законом** от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон).

2. В настоящих Требованиях используются следующие основные понятия, определенные в **статье 2** Федерального закона:

1) **электронная подпись** (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) **удостоверяющий центр** (далее - УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом;

3) **ключ ЭП** - уникальная последовательность символов, предназначенная для создания ЭП;

4) **ключ проверки ЭП** - уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее - проверка ЭП);

5) **средства ЭП** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП;

6) **сертификат ключа проверки ЭП** - электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

3. Настоящие Требования устанавливают структуру и содержание требований к средствам **ЭП**.

4. Настоящие Требования предназначены для заказчиков и разработчиков разрабатываемых (модернизируемых) средств ЭП при их взаимодействии между собой, с организациями, проводящими криптографические, инженерно-криптографические и специальные исследования средств ЭП, ФСБ России, осуществляющей подтверждение соответствия средств ЭП настоящим Требованиям.

5. Настоящие Требования распространяются на средства ЭП, предназначенные для использования на территории Российской Федерации, в учреждениях Российской Федерации за рубежом и в находящихся за рубежом обособленных подразделениях юридических лиц, образованных в соответствии с законодательством Российской Федерации.

6. К средствам ЭП в части их разработки, производства, реализации и эксплуатации предъявляются требования, закрепленные Положением о разработке,

производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (**Положение ПКЗ-2005**), утвержденным **приказом** ФСБ России от 9 февраля 2005 г. № 66***(1)** (с **изменениями**, внесенными **приказом** ФСБ России от 12 апреля 2010 г. № 173***(2)**, для шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

7. Требования к технологиям создания (формирования) и проверки ЭП с помощью средства ЭП указываются в тактико-техническом задании или техническом задании на проведение опытно-конструкторской работы или составной части опытно-конструкторской работы по разработке (модернизации) средства ЭП (далее - ТЗ на разработку (модернизацию) средства ЭП).

## II. Требования к средствам ЭП

8. При создании **ЭП** средства ЭП должны:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает***(3)**;
- создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП***(3)**;
- однозначно показывать, что ЭП создана***(3)**.

9. При проверке ЭП средства ЭП должны:

- показывать содержание электронного документа, подписанного ЭП***(3)**;
- показывать информацию о внесении изменений в подписанный ЭП электронный документ***(3)**;
- указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы***(3)**.

10. Требования **пунктов 8** и **9** настоящих Требований не применяются к средствам ЭП, используемым для автоматического создания и (или) автоматической проверки ЭП в информационной системе.

11. Средство ЭП должны противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой средством ЭП информации или с целью создания условий для этого (далее - атака).

12. В зависимости от способностей противостоять атакам средства ЭП подразделяются на классы***(4)**.

13. Средства ЭП **класса КС1** противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

13.1. Самостоятельное осуществление создания способов атак, подготовки и проведения атак.

13.2. Действия на различных этапах жизненного цикла средства ЭП***(5).**

13.3. Проведение атаки только извне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона***(6)**.

13.4. Проведение на этапах разработки, производства, хранения, транспортировки средств ЭП и этапе ввода в эксплуатацию средств ЭП (пусконаладочные работы) следующих атак:

- внесение несанкционированных изменений в средство ЭП и (или) в

компоненты СФ, в том числе с использованием вредоносных программ;

- внесение несанкционированных изменений в документацию на средство ЭП и на компоненты СФ.

13.5. Проведение атак на следующие объекты:

- документацию на средство ЭП и на компоненты СФ;
- защищаемые электронные документы;
- ключевую, аутентифицирующую и парольную информацию средства ЭП;
- средство ЭП и его программные и аппаратные компоненты;
- аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей инициализацию этих средств (далее - аппаратные компоненты СФ);
- программные компоненты СФ;
- данные, передаваемые по каналам связи;
- помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы средства ЭП и СФ;
- иные объекты атак, которые при необходимости указываются в ТЗ на разработку (модернизацию) средства ЭП с учетом используемых в информационной системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО).

13.6. Получение следующей информации:

- общих сведений об информационной системе, в которой используется средство ЭП (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);
- сведений об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно со средством ЭП;
- сведений о физических мерах защиты объектов, в которых размещены средства ЭП;
- сведений о мерах по обеспечению контролируемой зоны объектов информационной системы, в которой используется средство ЭП;
- сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы средства ЭП и СФ;
- содержания находящейся в свободном доступе документации на аппаратные и программные компоненты средства ЭП и СФ;
- общих сведений о защищаемой информации, используемой в процессе эксплуатации средства ЭП;
- всех возможных данных, передаваемых в открытом виде по каналам связи, не защищенным от несанкционированного доступа (далее - НСД) к информации организационно-техническими мерами;
- сведений о линиях связи, по которым передается защищаемая средством ЭП информация;
- сведений обо всех проявляющихся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушениях правил эксплуатации средства ЭП и СФ;
- сведений обо всех проявляющихся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправностях и сбоях

аппаратных компонентов средства ЭП и СФ;

- сведений, получаемых в результате анализа любых сигналов от аппаратных компонентов средства ЭП и СФ, которые может перехватить нарушитель.

13.7. Использование:

- находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты средства ЭП и СФ;

- специально разработанных АС и ПО.

13.8. Использование в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки (далее - канал атаки):

- не защищенных от НСД к информации организационно-техническими мерами каналов связи (как вне контролируемой зоны, так и в ее пределах), по которым передается защищаемая средством ЭП информация;

- каналов распространения сигналов, сопровождающих функционирование средства ЭП и СФ.

13.9. Проведение атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц.

13.10. Использование АС и ПО из состава средств информационной системы, используемых на местах эксплуатации средства ЭП (далее - штатные средства) и находящихся за пределами контролируемой зоны.

14. Средства **ЭП класса КС2** противостоят атакам, при создании способов, подготовке и проведении которых используются возможности, перечисленные в **подпунктах 13.1 - 13.10** настоящих Требований, и следующие дополнительные возможности:

14.1. Проведение атаки при нахождении, как вне пределов, так и в пределах контролируемой зоны.

14.2. Использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется средство ЭП, и направленными на предотвращение и пресечение несанкционированных действий.

15. Средства ЭП **класса КС3** противостоят атакам, при создании способов, подготовке и проведении которых используются возможности, перечисленные в **подпунктах 13.1 - 13.10**, **14.1**, **14.2** настоящих Требований, и следующие дополнительные возможности:

15.1. Доступ к СВТ, на которых реализованы средство ЭП и СФ.

15.2. Возможность располагать аппаратными компонентами средства ЭП и СФ в объеме, зависящем от мер, направленных на предотвращение и пресечение несанкционированных действий, реализованных в информационной системе, в которой используется средство ЭП.

16. Средства ЭП **класса КВ1** противостоят атакам, при создании способов, подготовке и проведении которых используются возможности, перечисленные в **подпунктах 13.1 - 13.10**, **14.1**, **14.2**, **15.1**, **15.2** настоящих Требований, и следующие дополнительные возможности:

16.1. Создание способов атак, подготовка и проведение атак с привлечением специалистов, имеющих опыт разработки и анализа средств ЭП, включая специалистов в области анализа сигналов, сопровождающих функционирование средства ЭП и СФ.

16.2. Проведение лабораторных исследований средства ЭП, используемого вне контролируемой зоны, в объеме, зависящем от мер, направленных на предотвращение и пресечение несанкционированных действий, реализованных в информационной системе, в которой используется средство ЭП.

17. Средства ЭП **класса КВ2** противостоят атакам, при создании способов, подготовке и проведении которых используются возможности, перечисленные в **подпунктах 13.1 - 13.10**, **14.1**, **14.2**, **15.1**, **15.2**, **16.1**, **16.2** настоящих Требований, и следующие дополнительные возможности:

17.1. Создание способов атак, подготовка и проведение атак с привлечением специалистов, имеющих опыт разработки и анализа средств ЭП, включая специалистов в области использования для реализации атак возможностей прикладного ПО, не описанных в документации на прикладное ПО.

17.2. Постановка работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств ЭП и СФ.

17.3. Возможность располагать исходными текстами входящего в СФ прикладного ПО.

18. Средства ЭП **класса КА1** противостоят атакам, при создании способов, подготовке и проведении которых используются возможности, перечисленные в **подпунктах 13.1 - 13.10**, **14.1**, **14.2**, **15.1**, **15.2**, **16.1**, **16.2**, **17.1 - 17.3** настоящих Требований, и следующие дополнительные возможности:

18.1. Создание способов атак, подготовка и проведение атак с привлечением специалистов, имеющих опыт разработки и анализа средств ЭП, включая специалистов в области использования для реализации атак возможностей системного ПО, не описанных в документации на системное ПО.

18.2. Возможность располагать всей документацией на аппаратные и программные компоненты СФ.

18.3. Возможность располагать всеми аппаратными компонентами средства ЭП и СФ.

19. В случае реализации в средстве **ЭП** функции проверки ЭП электронного документа с использованием сертификата ключа проверки ЭП эта реализация должна исключить возможность проверки ЭП электронного документа без проверки ЭП в сертификате ключа проверки ЭП или без наличия положительного результата проверки ЭП в сертификате ключа проверки ЭП.

20. При разработке средств ЭП должны использоваться криптографические алгоритмы, утвержденные в качестве государственных стандартов или имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований***(7)**.

21. Инженерно-криптографическая защита средства ЭП должна исключить события, приводящие к возможности проведения успешных атак в условиях возможных неисправностей или сбоев аппаратного компонента средства ЭП или аппаратного компонента СВТ, на котором реализовано программное средство ЭП.

22. В средстве ЭП должны быть реализованы только заданные в ТЗ на разработку (модернизацию) средства ЭП алгоритмы функционирования средства ЭП.

23. Программный компонент средства ЭП (в случае наличия программного компонента средства ЭП) должен удовлетворять следующим требованиям:

- объектный (загрузочный) код программного компонента средства ЭП должен

соответствовать его исходному тексту;

- в программном компоненте средства ЭП должны использоваться при реализации только описанные в документации функции программной среды, в которой функционирует средство ЭП;

- в исходных текстах программного компонента средства ЭП должны отсутствовать возможности, позволяющие модифицировать или искажать алгоритм работы средства ЭП в процессе его использования, модифицировать или искажать информационные или управляющие потоки и процессы, связанные с функционированием средства ЭП, и получать нарушителям доступ к хранящейся в открытом виде ключевой, идентификационной и (или) аутентифицирующей информации средства ЭП;

- значения входных и внутренних параметров, а также значения параметров настроек программного компонента средства ЭП не должны негативно влиять на его функционирование.

24. В случае планирования размещения средств ЭП в помещениях, в которых присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, АС иностранного производства, входящие в состав средств ЭП, должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

В случае планирования размещения средств ЭП в помещениях, в которых отсутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и не установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну:

- решение о проведении проверок АС иностранного производства, входящих в состав средств ЭП **классов КС1, КС2, КС3, КВ1 и КВ2**, принимается организацией, обеспечивающей эксплуатацию данных средств ЭП;

- проверки АС иностранного производства, входящих в состав средств ЭП **класса КА1**, проводятся в обязательном порядке.

25. Средство ЭП должно проводить аутентификацию субъектов доступа (лиц, процессов) к этому средству, при этом:

- при осуществлении доступа к средству ЭП аутентификация субъекта доступа должна проводиться до начала выполнения первого функционального модуля средства ЭП;

- механизмы аутентификации должны блокировать доступ этих субъектов к функциям средства ЭП при отрицательном результате аутентификации.

26. Средство ЭП должно проводить аутентификацию лиц, осуществляющих локальный доступ к средству ЭП.

27. Необходимость проведения средством ЭП аутентификации процессов, осуществляющих локальный или удаленный (сетевой) доступ к средству ЭП, указывается в ТЗ на разработку (модернизацию) средства ЭП.

28. Для любого входящего в средство ЭП механизма аутентификации должен быть реализован механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно быть больше 10. При превышении числа следующих подряд попыток аутентификации одного субъекта

доступа установленного предельного значения доступ этого субъекта к средству ЭП должен блокироваться на заданный в ТЗ на разработку (модернизацию) средства ЭП промежуток времени.

29. В средстве ЭП должен быть реализован механизм (процедура) контроля целостности средства ЭП и СФ.

Контроль целостности может осуществляться:

- в начале работы со средством ЭП до перехода СВТ, в котором реализовано средство ЭП, в рабочее состояние (например, до загрузки операционной системы СВТ);

- в ходе регламентных проверок средства ЭП на местах эксплуатации (регламентный контроль);

- в автоматическом режиме в процессе функционирования средства ЭП (динамический контроль).

Контроль целостности должен проводиться в начале работы со средством ЭП.

Механизм регламентного контроля целостности должен входить в состав средств ЭП.

30. Для средств **ЭП классов КС1 и КС2** необходимость предъявления требований к управлению доступом и очистке памяти, а также их содержание указываются в ТЗ на разработку (модернизацию) средства ЭП.

31. В состав средств ЭП **классов КС3, КВ1, КВ2 и КА1 или СФ** должны входить компоненты, обеспечивающие:

- управление доступом субъектов к различным компонентам и (или) целевым функциям средства ЭП и СФ на основе параметров, заданных администратором или производителем средства ЭП (требования к указанному компоненту определяются и обосновываются организацией, проводящей исследования средства ЭП с целью оценки соответствия средства ЭП настоящим Требованиям);

- очистку оперативной и внешней памяти, используемой средством ЭП для хранения защищаемой информации, при освобождении (перераспределении) памяти путем записи маскирующей информации (случайной или псевдослучайной последовательности символов) в память.

32. В состав средств ЭП **классов КВ2 и КА1 или СФ** должны входить компоненты, обеспечивающие экстренное стирание защищаемой информации ограниченного доступа. Требования к реализации и надежности стирания задаются в ТЗ на разработку (модернизацию) средства ЭП.

33. Для средств ЭП **классов КС1 и КС2** необходимость предъявления требований к регистрации событий и их содержание указываются в ТЗ на разработку (модернизацию) средства ЭП.

34. В состав средств ЭП **классов КС3, КВ1, КВ2 и КА1** должен входить модуль, производящий фиксацию в электронном журнале регистрации событий в средстве ЭП и СФ, связанных с выполнением средством ЭП своих целевых функций.

Требования к указанному модулю и перечень регистрируемых событий определяются и обосновываются организацией, проводящей исследования средства ЭП с целью оценки соответствия средства ЭП настоящим Требованиям.

35. Журнал регистрации событий должен быть доступен только лицам, определенным оператором информационной системы, в которой используется средство ЭП, или уполномоченными им лицами. При этом доступ к журналу регистрации событий должен осуществляться только для просмотра записей и для

перемещения содержимого журнала регистрации событий на архивные носители.

36. Срок действия ключа проверки ЭП не должен превышать срок действия ключа ЭП более чем на 15 лет.

37. Требования к механизму контроля срока использования ключа ЭП, блокирующего работу средства ЭП в случае попытки использования ключа дольше заданного срока, определяются разработчиком средства ЭП и обосновываются организацией, проводящей исследования средства ЭП с целью оценки соответствия средства ЭП настоящим Требованиям.

38. Криптографические протоколы, обеспечивающие операции с ключевой информацией средства ЭП, должны быть реализованы непосредственно в средстве ЭП.

39. Исследования средств ЭП с целью оценки соответствия средств ЭП настоящим Требованиям должны проводиться с использованием разрабатываемых ФСБ России числовых значений параметров и характеристик реализуемых в средствах ЭП механизмов защиты и аппаратных и программных компонентов СФ***(8)**.

---

*(1) Зарегистрирован Минюстом России 3 марта 2005 г., регистрационный № 6382.

*(2) Зарегистрирован Минюстом России 25 мая 2010 г., регистрационный № 17350.

*(3) Реализуется в том числе с использованием аппаратных и программных средств, совместно с которыми штатно функционируют средства ЭП и которые способны повлиять на выполнение предъявляемых к средствам ЭП требований, в совокупности представляющих среду функционирования средств ЭП (далее - СФ).

*(4) Необходимый класс разрабатываемого (модернизируемого) средства ЭП определяется заказчиком (разработчиком) средства ЭП путем определения возможностей осуществлять создание способов атак, подготовку и проведение атак на основе **пунктов 13-18** настоящих Требований и указывается в ТЗ на разработку (модернизацию) средства ЭП.

*(5) К этапам жизненного цикла средства ЭП относятся разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация.

*(6) Границей контролируемой зоны могут быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

*(7) **Подпункт 25 пункта 9** Положения о Федеральной службе безопасности Российской Федерации, утвержденного **Указом** Президента Российской Федерации от 11 августа 2003 г. № 960 (Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2004, № 28, ст. 2883; 2005, № 36, ст. 3665; № 49, ст. 5200; 2006, № 25, ст. 2699; № 31 (ч. I), ст. 3463; 2007, № 1 (ч. I), ст. 205; № 49, ст. 6133; № 53, ст. 6554; 2008, № 36, ст. 4087; № 43, ст. 4921; № 47, ст. 5431; 2010, № 17, ст. 2054; № 20, ст. 2435; 2011, № 2, ст. 267; № 9, ст. 1222) (далее - Положение о ФСБ России).

*(8) **Подпункт 47 пункта 9** Положения о ФСБ России.

**Приложение № 2**
**к приказу ФСБ**
**от 27 декабря 2011 г. № 796**

# Требования к средствам удостоверяющего центра

## I. Общие положения

1. Настоящие Требования разработаны в соответствии с **Федеральным законом** от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон).

2. В настоящих Требованиях используются следующие основные понятия, определенные в **статье 2** Федерального закона:

1) **электронная подпись** (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

2) **удостоверяющий центр** (далее - УЦ) - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом;

3) **средства ЭП** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП;

4) **ключ ЭП** - уникальная последовательность символов, предназначенная для создания ЭП;

5) **ключ проверки ЭП** - уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее - проверка ЭП);

6) **сертификат ключа проверки ЭП** - электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом УЦ и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

7) **квалифицированный сертификат ключа проверки ЭП** (далее - квалифицированный сертификат) - сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП (далее - уполномоченный федеральный орган);

8) **владелец сертификата ключа проверки ЭП** - лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки ЭП;

9) **аккредитация УЦ** - признание уполномоченным федеральным органом соответствия УЦ требованиям Федерального закона;

10) **средства УЦ** - аппаратные и (или) программные средства, используемые для реализации функций УЦ;

11) **участники электронного взаимодействия** - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

3. Настоящие Требования устанавливают структуру и содержание требований к

средствам УЦ.

4. Настоящие Требования предназначены для заказчиков и разработчиков разрабатываемых (модернизируемых) средств УЦ при их взаимодействии между собой, с организациями, проводящими криптографические, инженерно-криптографические и специальные исследования средств УЦ, ФСБ России, осуществляющей подтверждение соответствия средств УЦ настоящим Требованиям.

5. Настоящие Требования распространяются на средства УЦ, предназначенные для использования на территории Российской Федерации.

6. К средствам УЦ в части их разработки, производства, реализации и эксплуатации предъявляются требования, закрепленные Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (**Положение ПКЗ-2005**), утвержденным **приказом** ФСБ России от 9 февраля 2005 г. № 66***(1)** (с **изменениями**, внесенными **приказом** ФСБ России от 12 апреля 2010 г. № 173***(2)**, для шифровальных (криптографических) средств защиты информации (далее - СКЗИ) с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

## II. Требования к средствам УЦ

7. Средства УЦ должны противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения инженерно-технической и криптографической безопасности средств УЦ или с целью создания условий для этого (далее - атака).

8. В зависимости от способностей противостоять атакам средства УЦ подразделяются на классы*(3).

9. Средства УЦ **класса КС1** противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

9.1. Подготовка и проведение атак извне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона).

9.2. Подготовка и проведение атак без использования доступа к функциональным возможностям программно-аппаратных средств взаимодействия с УЦ.

9.3. Самостоятельное осуществление создания способов атак, подготовки и проведения атак на следующие объекты:

- документацию на средства УЦ;
- защищаемые электронные документы;
- ключевую, аутентифицирующую и парольную информацию;
- средства УЦ, их программные и аппаратные компоненты;
- данные, передаваемые по каналам связи;
- помещения, в которых находятся аппаратные средства (далее - АС), на которых реализованы средства УЦ, а также другие защищаемые ресурсы информационной системы.

9.4. Внесение на этапах разработки, производства, хранения, транспортировки и ввода в эксплуатацию средств УЦ:

- негативных функциональных возможностей в средства УЦ, в том числе с

использованием вредоносных программ;

- несанкционированных изменений в документацию на средства УЦ.

9.5. Получение следующей информации:

- общих сведений об информационной системе, в которой используются средства УЦ (назначение, состав, объекты, в которых размещены ресурсы информационной системы);

- сведений об информационных технологиях, базах данных, АС, программном обеспечении (далее - ПО), используемых в информационной системе совместно со средствами УЦ;

- сведений о физических мерах защиты объектов, в которых размещены средства УЦ;

- сведений о мерах по обеспечению защиты контролируемой зоны объектов информационной системы, в которой используются средства УЦ;

- сведений о мерах по разграничению доступа в помещения, в которых размещены средства УЦ;

- содержания находящейся в свободном доступе технической документации на средства УЦ;

- сведений о защищаемой информации, используемой в процессе эксплуатации средств УЦ (виды защищаемой информации: служебная информация, парольная и аутентифицирующая информация, конфигурационная информация, управляющая информация, информация в электронных журналах регистрации; общие сведения о содержании каждого вида защищаемой информации; характеристики безопасности для каждого вида защищаемой информации);

- всех возможных данных, передаваемых в открытом виде по каналам связи, не защищенным от несанкционированного доступа (далее - НСД) к информации организационно-техническими мерами;

- сведений о линиях связи, по которым передается защищаемая с использованием средств УЦ информация;

- сведений обо всех проявляющихся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушениях правил эксплуатации средств УЦ;

- сведений обо всех проявляющихся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправностях и сбоях средств УЦ;

- сведений, получаемых в результате анализа любых доступных для перехвата сигналов от аппаратных компонентов средств УЦ.

9.6. Использование:

- находящихся в свободном доступе или за пределами контролируемой зоны АС и ПО, включая программные и аппаратные компоненты средств УЦ;

- специально разработанных АС и ПО.

9.7. Использование в качестве каналов атак не защищенных от НСД к информации организационно-техническими мерами каналов связи (как вне контролируемой зоны, так и в ее пределах), по которым передается информация, обрабатываемая средствами УЦ.

10. Средства УЦ **класса КС2** противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

10.1. Возможности, перечисленные в **подпунктах 9.3 - 9.7** настоящих

Требований.

10.2. Подготовка и проведение атак из контролируемой зоны.

10.3. Подготовка и проведение атак без использования доступа к АС, на которых реализованы средства УЦ.

10.4. Использование штатных средств информационной системы, в которой используются средства УЦ.

11. Средства УЦ **класса КС3** противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

11.1. Возможности, перечисленные в **подпунктах 10.1**, **10.4** настоящих Требований.

11.2. Подготовка и проведение атак из-за пределов контролируемой зоны с использованием доступа к функциональным возможностям программно-аппаратных средств взаимодействия с УЦ на основе легального обладания аутентифицирующей информацией либо подготовка и проведение атак из контролируемой зоны с использованием доступа к АС, на которых реализованы компоненты УЦ, с правами лица, не являющегося членом группы физических лиц, уполномоченных производить инсталляцию, конфигурирование и эксплуатацию средств УЦ, конфигурирование профиля и параметров журнала аудита (функции системного администратора), архивирование, резервное копирование и восстановление информации после сбоев (функции оператора), создание и аннулирование сертификатов ключей проверки **ЭП** (функции администратора сертификации), просмотр и поддержку журнала аудита (функции администратора аудита) (далее - группа администраторов средств УЦ) ни одного из компонентов УЦ.

11.3. Обладание АС УЦ в объеме, зависящем от реализованных мер, направленных на предотвращение и пресечение несанкционированных действий.

12. Средства УЦ **класса КВ1** противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

12.1. Возможности, перечисленные в **подпунктах 11.1 - 11.3** настоящих Требований.

12.2. Осуществление создания способов и подготовки атак с привлечением специалистов, имеющих опыт разработки и анализа СКЗИ УЦ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочных электромагнитных излучений и наводок СКЗИ УЦ).

12.3. Проведение лабораторных исследований средств УЦ, используемых вне контролируемой зоны в объеме, зависящем от реализованных мер, направленных на предотвращение и пресечение несанкционированных действий.

13. Средства УЦ класса КВ2 противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

13.1. Возможности, перечисленные в **подпунктах 12.1-12.3** настоящих Требований.

13.2. Осуществление создания способов и подготовки атак с привлечением специалистов в области использования для реализации атак не декларированных возможностей прикладного и системного ПО.

13.3. Постановка работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа средств УЦ.

13.4. Обладание исходными текстами прикладного ПО, применяемого в

информационной системе, в которой используются средства УЦ, и находящейся в свободном доступе документацией.

14. Средства УЦ **класса КА1** противостоят атакам, при создании способов, подготовке и проведении которых используются следующие возможности:

14.1. Возможности, перечисленные в **подпунктах 13.1 - 13.4** настоящих Требований.

14.2. Осуществление создания способов и подготовки атак с привлечением научно-исследовательских центров, специализирующихся в области разработки и анализа СКЗИ и в области использования для реализации атак не декларированных возможностей прикладного и системного ПО.

14.3. Обладание всей документацией на аппаратные и программные компоненты средств УЦ.

14.4. Обладание всеми аппаратными компонентами средств УЦ.

15. Средства УЦ должны эксплуатироваться в соответствии с эксплуатационной документацией на средства УЦ. Комплекс организационно-технических мероприятий по обеспечению безопасного функционирования средств УЦ должен быть указан в эксплуатационной документации на средства УЦ.

16. Класс средств **ЭП**, используемых в средствах УЦ, должен быть не ниже соответствующего класса средств УЦ. Класс средств ЭП, используемых в средствах УЦ, должен быть указан в эксплуатационной документации на средства УЦ.

Класс СКЗИ, используемых в средствах УЦ, должен быть не ниже соответствующего класса средств УЦ. Класс СКЗИ, используемых в средствах УЦ, должен быть указан в эксплуатационной документации на средства УЦ.

17. Каждое требование, предъявляемое к средствам УЦ любого класса кроме КА1, либо предъявляется к средствам УЦ следующего класса без изменений (в этом случае оно в перечне требований к средствам УЦ следующего класса не указывается), либо ужесточается (в этом случае в перечне требований к средствам УЦ следующего класса приводится ужесточенная формулировка). Требования к средствам УЦ следующего класса могут содержать дополнительные требования, не входящие в требования к средствам УЦ предыдущего класса.

18. Требования к ПО средств УЦ:

18.1. Требования для средств УЦ **класса КС1**:

- ПО средств УЦ не должно содержать средств, позволяющих модифицировать или искажать алгоритм работы программных средств и АС УЦ.

18.2. Требования для средств УЦ **класса КС2**:

- прикладное ПО средств УЦ и СКЗИ, используемых в УЦ, должно использовать только документированные функции системного ПО.

18.3. Требования для средств УЦ **класса КС3**:

- системное и прикладное ПО средств УЦ должно обеспечивать разграничение доступа системного администратора средств УЦ, администратора сертификации средств УЦ и лиц, обеспечиваемых системным администратором средств УЦ идентифицирующей и аутентифицирующей информацией и не являющихся администратором сертификации средств УЦ (далее - пользователи средств УЦ), к информации, обрабатываемой средствами УЦ, на основании правил разграничения доступа, заданных системным администратором средств УЦ;

- системное и прикладное ПО средств УЦ должно соответствовать **4 уровню контроля** отсутствия не декларированных возможностей;

- системное и прикладное ПО средств УЦ не должно содержать известных уязвимостей, опубликованных в общедоступных источниках;

- в состав системного и (или) прикладного ПО средств УЦ должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа.

18.4. Требования для средств УЦ **класса КВ1** совпадают с требованиями для средств УЦ **класса КС3**.

18.5. Требования для средств УЦ **класса КВ2**:

- исходные тексты системного и прикладного ПО средств УЦ должны пройти проверку реализации в них методов и способов защиты информации, противостоящих атакам, для подготовки и проведения которых используются возможности, перечисленные в **пунктах 9-13** настоящих Требований;

- исходные тексты системного и прикладного ПО должны пройти проверку на отсутствие не декларированных возможностей;

- системное и прикладное ПО должно быть устойчиво к компьютерным атакам из внешних сетей.

18.6. Требования для средств УЦ **класса КА1**:

- исходные тексты системного и прикладного ПО средств УЦ должны пройти формальную верификацию реализации в них методов и способов защиты информации, противостоящих атакам, для подготовки и проведения которых используются возможности, перечисленные в **пунктах 9-14** настоящих Требований, а также отсутствия в них не декларированных возможностей.

19. Требования к АС УЦ:

19.1. В случае планирования размещения АС УЦ в помещениях, в которых присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены технические средства и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, технические средства иностранного производства, входящие в состав средств УЦ, должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации, а также исследованиям на соответствие требованиям по защите от утечки информации по каналам побочных электромагнитных излучений и наводок в соответствии с категорией выделенного помещения.

19.2. Требования для средств УЦ **класса КС1**:

- проводится проверка соответствия реализации целевых функций УЦ на основе системы тестов АС УЦ.

19.3. Требования для средств УЦ **классов КС2, КС3, КВ1, КВ2** совпадают с требованиями для средств УЦ **класса КС1**.

19.4. Требования для средств УЦ **класса КА1**:

- проведение специальной проверки технических средств иностранного производства, входящих в состав АС УЦ, в целях выявления устройств, предназначенных для негласного получения информации;

- проведение полной верификации АС (совместно с анализом программного кода BIOS), на которых реализуются средства УЦ, с целью исключения негативных функциональных возможностей.

20. Требования к ролевому разграничению:

20.1. Для обеспечения выполнения функций УЦ средства УЦ должны

поддерживать ролевое разграничение членов группы администраторов средств УЦ.

20.2. Требования для средств УЦ **класса КС1**:

- должны быть определены список ролей и распределение обязанностей между ролями;

- список ролей и распределение обязанностей между ролями должны быть указаны в эксплуатационной документации на средства УЦ.

20.3. Требования для средств УЦ **класса КС2** совпадают с требованиями для средств УЦ класса КС1.

20.4. Требования для средств УЦ **класса КС3**:

- средства УЦ должны поддерживать следующие обязательные роли:

1) системного администратора с основными обязанностями инсталляции, конфигурации и поддержки функционирования средств УЦ, создания и поддержки профилей членов группы администраторов средств УЦ, конфигурации профиля и параметров журнала аудита;

2) администратора сертификации с основными обязанностями: создание и аннулирование сертификатов ключей проверки ЭП;

- в средствах УЦ должен быть реализован механизм, исключающий возможность авторизации одного члена из группы администраторов средств УЦ для выполнения различных ролей.

20.5. Требования для средств УЦ **класса КВ1**:

- средства УЦ должны обеспечивать наличие обязательной роли оператора с основными обязанностями по резервному копированию и восстановлению.

20.6. Требования для средств УЦ **класса КВ2** совпадают с требованиями для средств УЦ класса КВ1.

20.7. Требования для средств УЦ **класса КА1**:

- средства УЦ должны обеспечивать наличие обязательной роли администратора аудита с основными обязанностями: просмотр и поддержка журнала аудита;

- системный администратор не должен иметь возможности вносить изменения в журнал аудита.

21. Требования к целостности средств УЦ:

21.1. Средства УЦ должны содержать механизм контроля несанкционированного случайного и (или) преднамеренного искажения (изменения, модификации) и (или) разрушения информации, программных средств и АС УЦ (далее - механизм контроля целостности).

21.2. Требования для средств УЦ **класса КС1**:

- требования к механизму контроля целостности должны быть указаны в ТЗ на разработку (модернизацию) средств УЦ;

- должен быть определен период контроля целостности программных средств и АС УЦ и указан в эксплуатационной документации на средства УЦ;

- контроль целостности программных средств и АС УЦ должен выполняться при каждой перезагрузке операционной системы (далее - ОС);

- должны иметься средства восстановления целостности средств УЦ.

21.3. Требования для средств УЦ **класса КС2** совпадают с требованиями для средств УЦ класса КС1.

21.4. Требования для средств УЦ **класса КС3**:

- контроль целостности должен выполняться не реже одного раза в сутки.

21.5. Требования для средств УЦ **класса КВ1**:

- контроль целостности должен выполняться до загрузки ОС средств УЦ.

21.6. Требования для средств УЦ **класса КВ2** совпадают с требованиями для средств УЦ класса КВ1.

21.7. Требования для средств УЦ **класса КА1**:

- контроль целостности должен осуществляться динамически при функционировании средств УЦ.

22. Требования к управлению доступом:

22.1. Средства УЦ должны обеспечивать управление доступом.

22.2. Требования для средств УЦ **класса КС1**:

- должны быть определены требования к управлению доступом и указаны в ТЗ на разработку (модернизацию) средств УЦ.

22.3. Требования для средств УЦ **класса КС2** совпадают с требованиями для средств УЦ класса КС1.

22.4. Требования для средств УЦ **класса КС3**:

- в УЦ должен обеспечиваться дискреционный принцип контроля доступа.

22.5. Требования для средств УЦ **класса КВ1** совпадают с требованиями для средств УЦ класса КС3.

22.6. Требования для средств УЦ **класса КВ2**:

должно быть обеспечено создание замкнутой рабочей среды***(4)** средств УЦ.

22.7. Требования для средств УЦ **класса КА1**:

- в УЦ должен обеспечиваться мандатный принцип контроля доступа;

- для ввода ключа ЭП администратора сертификации требуется не менее двух доверенных лиц***(5)**.

23. Требования к идентификации и аутентификации:

23.1. Идентификация и аутентификация включают в себя распознавание пользователя средств УЦ, члена группы администраторов средств УЦ или процесса и проверку их подлинности. Механизм аутентификации должен блокировать доступ этих субъектов к функциям УЦ при отрицательном результате аутентификации.

23.2. В средствах УЦ для любой реализованной процедуры аутентификации должен быть применен механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно быть больше трех. При превышении числа следующих подряд попыток аутентификации одного субъекта доступа установленного предельного значения доступ этого субъекта доступа к средствам УЦ должен быть заблокирован на промежуток времени, который указывается в ТЗ на разработку (модернизацию) средств УЦ.

23.3. Требования для средств УЦ **класса КС1**:

- описание процедуры регистрации пользователей средств УЦ (внесения данных в реестр пользователей средств УЦ) должно содержаться в эксплуатационной документации на средства УЦ;

- для всех лиц, осуществляющих доступ к средствам УЦ, должна проводиться аутентификация. При этом допускается ограничиться использованием для аутентификации только символьного периодически изменяющегося пароля из не менее чем 8 символов при мощности алфавита не менее 36 символов. Период изменения пароля не должен быть больше 6 месяцев.

23.4. Требования для средств УЦ **класса КС2**:

- необходимость предъявления пользователем средств УЦ при его регистрации

документов, удостоверяющих личность, должна быть отражена в эксплуатационной документации на средства УЦ;

- для всех пользователей средств УЦ допускается использование механизмов удаленной аутентификации. Специальные характеристики механизмов удаленной аутентификации должны быть подтверждены в рамках проведения проверки соответствия средств УЦ и объектов информатизации, использующих данные средства, настоящим Требованиям;

- при осуществлении локального доступа к средствам УЦ аутентификация членов группы администраторов средств УЦ должна выполняться до перехода в рабочее состояние этих средств УЦ (например, до загрузки базовой ОС).

23.5. Требования для средств УЦ **класса КС3**:

- в средствах УЦ должен быть реализован механизм аутентификации локальных пользователей, имеющих доступ к средствам УЦ, но не входящих в состав группы администраторов средств УЦ.

23.6. Требования для средств УЦ **класса КВ1**:

- при осуществлении удаленного доступа к средствам УЦ использование только символьного пароля не допускается, должны использоваться механизмы аутентификации на основе криптографических протоколов.

23.7. Требования для средств УЦ **класса КВ2** совпадают с требованиями для средств УЦ **класса КВ1**.

23.8. Требования для средств УЦ **класса КА1**:

- в средствах УЦ для любого реализованного механизма аутентификации должна быть реализована возможность установки предельно допустимого количества следующих подряд попыток аутентификации одного субъекта доступа и установки времени блокировки доступа к средствам УЦ на местах их эксплуатации.

24. Требования к защите данных, поступающих (экспортируемых) в (из) УЦ:

24.1. Средства УЦ должны обеспечивать доверенный ввод самоподписанного сертификата ключа проверки ЭП.

24.2. Требования для средств УЦ **класса КС1**:

- средства УЦ должны обеспечивать передачу данных, содержащих информацию ограниченного доступа, поступающих в УЦ и экспортируемых из УЦ, способом, защищенным от НСД;

- в средствах УЦ должна быть реализована процедура защиты от навязывания ложных сообщений***(6)**;

- требования к процедуре защиты от навязывания ложных сообщений указываются в ТЗ на разработку (модернизацию) средств УЦ.

24.3. Требования для средств УЦ **класса КС2**:

- средства УЦ должны обеспечивать защиту первоначального запроса на сертификат ключа проверки ЭП;

- средства УЦ должны принимать критичную для функционирования УЦ информацию, только если она подписана ЭП.

24.4. Требования для средств УЦ **класса КС3**:

- в средствах УЦ должен быть реализован механизм защиты от навязывания ложных сообщений на основе использования средств **ЭП**, получивших подтверждение соответствия требованиям к средствам ЭП.

24.5. Требования для средств УЦ **класса КВ1**:

- в средствах УЦ должен быть реализован механизм защиты данных при

передаче их между физически разделенными компонентами на основе использования СКЗИ.

24.6. Требования для средств УЦ **классов КВ2 и КА1** совпадают с требованиями для средств УЦ **класса КВ1**.

25. Требования к регистрации событий:

25.1. Базовая ОС средств УЦ должна поддерживать ведение журнала аудита системных событий.

25.2. Требования для средств УЦ **класса КС1**:

- в средствах УЦ должен быть реализован механизм, производящий выборочную регистрацию событий в журнале аудита, связанных с выполнением УЦ своих функций;

- список регистрируемых событий должен содержаться в эксплуатационной документации на средства УЦ.

25.3. Требования для средств УЦ **класса КС2** совпадают с требованиями для средств УЦ **класса КС1**.

25.4. Требования для средств УЦ **класса КС3**:

- должны быть приняты меры обнаружения несанкционированных изменений журнала аудита пользователями средств УЦ, не являющимися членами группы администраторов средств УЦ.

25.5. Требования для средств УЦ **класса КВ1** совпадают с требованиями для средств УЦ **класса КС3**.

25.6. Требования для средств УЦ **класса КВ2**:

- должны быть приняты меры обнаружения несанкционированных изменений каждой записи в журнале аудита.

25.7. Требования для средств УЦ **класса КА1**:

- журнал аудита должен быть доступен только администратору аудита, который может осуществлять только его просмотр, копирование и полную очистку. После очистки первой записью в журнале аудита должен автоматически регистрироваться факт очистки с указанием даты, времени и информации о лице, производившем операцию.

26. Требования по надежности и устойчивости функционирования средств УЦ:

26.1. Должны быть определены требования по надежности и устойчивости функционирования средств УЦ и указаны в ТЗ на разработку (модернизацию) средств УЦ.

26.2. Требования для средств УЦ **класса КС1**:

- проводится расчет вероятности сбоев и неисправностей АС УЦ, приводящих к невыполнению УЦ своих функций.

26.3. Требования для средств УЦ **класса КС2**:

- должно осуществляться тестирование устойчивости функционирования средств УЦ.

26.4. Требования для средств УЦ **класса КС3**:

- должны быть определены требования по времени восстановления средств УЦ после сбоя и указаны в ТЗ на разработку (модернизацию) средств УЦ;

- меры и средства повышения надежности и устойчивости функционирования средств УЦ должны содержать механизмы квотирования ресурсов средств УЦ.

26.5. Требования для средств УЦ **класса КВ1**:

- вероятность сбоев и неисправностей АС УЦ, приводящих к невыполнению УЦ

своих функций, в течение суток не должна превышать аналогичной вероятности для используемых СКЗИ.

26.6. Требования для средств УЦ **классов КВ2 и КА1** совпадают с требованиями для средств УЦ **класса КВ1**.

27. Требования к ключевой информации:

27.1. Порядок создания, использования, хранения и уничтожения ключевой информации определяется в соответствии с требованиями эксплуатационной документации на средства ЭП и иные СКЗИ, используемые средствами УЦ.

27.2. Срок действия ключа ЭП средства ЭП, используемого средствами УЦ, должен соответствовать требованиям, установленным к средствам ЭП.

27.3. Требования для средств УЦ **класса КС1**:

- не допускается копирование информации ключевых документов (криптографических ключей, в том числе ключей ЭП) на носители (например, жесткий диск), не являющиеся ключевыми носителями, без ее предварительного шифрования (которое должно осуществляться встроенной функцией используемого СКЗИ). Копирование ключевых документов должно осуществляться только в соответствии с эксплуатационной документацией на используемое СКЗИ;

- ключи ЭП, используемые для подписи сертификатов ключей проверки ЭП и списков уникальных номеров сертификатов ключей проверки ЭП, действие которых на определенный момент было прекращено УЦ до истечения срока их действия (далее - список аннулированных сертификатов), не должны использоваться ни для каких иных целей;

- сроки действия всех ключей должны быть указаны в эксплуатационной документации на средства УЦ.

27.4. Требования для средств УЦ **классов КС2 и КС3** совпадают с требованиями для средств УЦ **класса КС1**.

27.5. Требования для средств УЦ **класса КВ1**:

- должны быть приняты организационно-технические меры, исключающие возможность компрометации ключа ЭП, используемого для подписи сертификатов ключей проверки ЭП и списков аннулированных сертификатов, при компрометации ключевой информации, доступной одному лицу.

27.6. Требования для средств УЦ **класса КВ2**:

- ключ ЭП, используемый для подписи сертификатов ключей проверки ЭП и списков аннулированных сертификатов, должен генерироваться, храниться, использоваться и уничтожаться в средстве ЭП. Допускается использование только средств ЭП, получивших подтверждение соответствия требованиям, предъявляемым к средствам ЭП в соответствии с Федеральным законом;

- должны быть приняты организационно-технические меры, исключающие возможность компрометации ключа ЭП, используемого для подписи сертификатов ключей проверки ЭП и списков аннулированных сертификатов, при компрометации ключевой информации, доступной двум лицам.

27.7. Требования для средств УЦ **класса КА1**:

- должны быть приняты организационно-технические меры, исключающие возможность компрометации ключа ЭП, используемого для подписи сертификатов ключей проверки ЭП и списков аннулированных сертификатов, при компрометации ключевой информации, доступной трем лицам.

28. Требования к резервному копированию и восстановлению

работоспособности средств УЦ:

28.1. Средства УЦ должны реализовывать функции резервного копирования и восстановления на случай повреждения АС и (или) информации, обрабатываемой средствами УЦ. В ходе резервного копирования должна быть исключена возможность копирования криптографических ключей.

28.2. Требования для средств УЦ **класса КС1**:

- данные, сохраненные при резервном копировании, должны быть достаточны для восстановления функционирования средств УЦ в состояние, зафиксированное на момент копирования.

28.3. Требования для средств УЦ **классов КС2 и КС3** совпадают с требованиями для средств УЦ **класса КС1**.

28.4. Требования для средств УЦ **класса КВ1**:

- должны быть приняты меры обнаружения несанкционированных изменений сохраненных данных;

- должны быть определены требования по времени восстановления и указаны в ТЗ на разработку (модернизацию) средств УЦ и в эксплуатационной документации на средства УЦ.

28.5. Требования для средств УЦ **класса КВ2**:

- сохраняемая при резервном копировании защищаемая информация должна сохраняться только в зашифрованном виде.

28.6. Требования для средств УЦ **класса КА1** совпадают с требованиями для средств УЦ **класса КВ2**.

29. Требования к созданию и аннулированию сертификатов ключей проверки **ЭП**:

29.1. Протоколы создания и аннулирования сертификатов ключей проверки ЭП должны быть описаны в эксплуатационной документации на средства УЦ.

29.2. Создаваемые УЦ сертификаты ключей проверки ЭП и списки аннулированных сертификатов должны соответствовать международным рекомендациям ITU-T X.509***(7)** (далее - рекомендации X.509). Все поля и дополнения, включаемые в сертификат ключей проверки ЭП и список аннулированных сертификатов, должны быть заполнены в соответствии с рекомендациями X.509. При использовании альтернативных форматов сертификатов ключей проверки ЭП должны быть определены требования к протоколам создания и аннулирования сертификатов ключей проверки ЭП и указаны в ТЗ на разработку (модернизацию) средств УЦ.

29.3. Средства УЦ должны реализовывать протокол аннулирования сертификата ключа проверки ЭП с использованием списков аннулированных сертификатов.

29.4. Допускается реализация протоколов аннулирования без использования списков аннулированных сертификатов, требования к которым должны быть указаны в ТЗ на разработку (модернизацию) средств УЦ.

29.5. Требования для средств УЦ **класса КС1**:

- в средствах УЦ должна быть реализована функция изготовления сертификата ключа проверки ЭП на бумажном носителе. Порядок выдачи сертификата ключа проверки ЭП на бумажном носителе, а также процедура контроля соответствия сертификата ключа проверки ЭП в электронном виде и на бумажном носителе должны быть указаны в эксплуатационной документации на средства УЦ;

- в средствах УЦ в отношении владельца сертификата ключа проверки ЭП должны быть реализованы механизмы проверки уникальности ключа проверки ЭП и обладания соответствующим ключом ЭП.

29.6. Требования для средств УЦ **класса КС2** совпадают с требованиями для средств УЦ **класса КС1**.

29.7. Требования для средств УЦ **класса КС3**:

- погрешность значений времени в сертификатах ключей проверки ЭП и списках аннулированных сертификатов не должна превышать 10 минут.

29.8. Требования для средств УЦ **класса КВ1**:

- погрешность значений времени в сертификатах ключей проверки ЭП и списках аннулированных сертификатов не должна превышать 5 минут.

29.9. Требования для средств УЦ **классов КВ2 и КА1** совпадают с требованиями для средств УЦ **класса КВ1**.

30. Требования к структуре сертификата ключа проверки ЭП и списка аннулированных сертификатов:

30.1. Требования для средств УЦ **класса КС1**:

- допустимые структуры сертификата ключа проверки ЭП и списка аннулированных сертификатов должны быть перечислены в эксплуатационной документации на средства УЦ;

- в средствах УЦ должен быть реализован механизм контроля соответствия создаваемых сертификатов ключей проверки ЭП и списков аннулированных сертификатов заданной структуре;

- в структуре сертификата ключа проверки ЭП должны быть предусмотрены поле, содержащее сведения о классе средств УЦ, с использованием которых был создан настоящий сертификат ключа проверки ЭП, и поле, содержащее сведения о классе средства ЭП владельца сертификата ключа проверки ЭП.

30.2. Требования для средств УЦ **классов КС2 и КС3** совпадают с требованиями для средств УЦ **класса КС1**.

30.3. Требования для средств УЦ **класса КВ1**:

- в средствах УЦ должен быть реализован механизм задания системным администратором набора допустимых дополнений сертификата ключа проверки ЭП и списка аннулированных сертификатов.

30.4. Требования для средств УЦ **классов КВ2 и КА1** совпадают с требованиями для средств УЦ **класса КВ1**.

31. Требования к реестру сертификатов ключей проверки ЭП и обеспечению доступа к нему:

31.1. Требования для средств УЦ **класса КС1**:

- в средствах УЦ должны быть реализованы механизмы хранения и поиска всех созданных сертификатов ключей проверки ЭП и списков аннулированных сертификатов в реестре, а также сетевого доступа к реестру.

31.2. Требования для средств УЦ **класса КС2** совпадают с требованиями для средств УЦ **класса КС1**.

31.3. Требования для средств УЦ **класса КС3**:

- в средствах УЦ должен быть реализован механизм поиска сертификатов ключей проверки ЭП и списков аннулированных сертификатов в реестре сертификатов ключей проверки ЭП по различным их атрибутам;

- все изменения реестра сертификатов ключей проверки ЭП должны

регистрироваться в журнале аудита.

31.4. Требования для средств УЦ **классов КВ1, КВ2 и КА1** совпадают с требованиями для средств УЦ **класса КС3**.

32. Требования к проверке ЭП в сертификате ключа проверки ЭП:

32.1. Должен быть определен механизм проверки подписи в сертификате ключа проверки ЭП по запросу участника электронного взаимодействия и указан в эксплуатационной документации на средства УЦ.

32.2. В средствах УЦ должен быть реализован механизм проверки подлинности ЭП УЦ в выдаваемых им сертификатах ключей проверки ЭП.

32.3. Проверка ЭП в сертификате ключа проверки ЭП осуществляется в соответствии с рекомендациями X.509, включая обязательную проверку всех критических дополнений.

32.4. Если, исходя из особенностей эксплуатации средств УЦ, допускается использование альтернативных форматов сертификата ключа проверки ЭП, должен быть определен механизм проверки подписи в сертификате ключа проверки ЭП и указан в ТЗ на разработку (модернизацию) средств УЦ.

33. Для ограничения возможностей по построению каналов атак на средства УЦ с использованием каналов связи должны применяться средства межсетевого экранирования.

34. Должны быть определены требования по защите средств УЦ от компьютерных вирусов и компьютерных атак и указаны в ТЗ на разработку (модернизацию) средств УЦ.

35. При подключении средств УЦ к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ **класса КВ2 или КА1**.

36. Исследования средств УЦ с целью подтверждения соответствия средств УЦ настоящим Требованиям должны проводиться с использованием разрабатываемых ФСБ России числовых значений параметров и характеристик механизмов защиты, реализуемых в средствах УЦ***(8)**.

---

*(1) Зарегистрирован Минюстом России 3 марта 2005 г., регистрационный № 6382.

*(2) Зарегистрирован Минюстом России 25 мая 2010 г., регистрационный № 17350.

*(3) Необходимый класс разрабатываемых (модернизируемых) средств УЦ определяется заказчиком (разработчиком) средств УЦ путем определения возможностей осуществлять создание способов атак, подготовку и проведение атак на основе **пунктов 9-14** настоящих Требований и указывается в тактико-техническом задании или техническом задании на проведение опытно-конструкторской работы или составной части опытно-конструкторской работы по разработке (модернизации) средств УЦ (далее - ТЗ на разработку (модернизацию) средств УЦ).

*(4) Программная среда, которая допускает существование в ней только фиксированного набора субъектов (программ, процессов).

*(5) Лица, являющиеся членами группы администраторов средств УЦ и заведомо не являющиеся нарушителями.

*(6) Навязывание ложного сообщения представляет собой действие, воспринимаемое участниками электронного взаимодействия или средствами УЦ как

передача истинного сообщения способом, защищенным от НСД.

*(7) ITU-T Recomme№datio№ X.509. Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks. 2008. http://www.itu.i№t/rec/T-REC-X.509-200811-i.

*(8) **Подпункт 47 пункта 9** Положения о Федеральной службе безопасности Российской Федерации, утвержденного **Указом** Президента Российской Федерации от 11 августа 2003 г. № 960 (Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2004, № 28, ст. 2883; 2005, № 36, ст. 3665; № 49, ст. 5200; 2006, № 25, ст. 2699; № 31 (ч. I), ст. 3463; 2007, № 1 (ч. I), ст. 205; № 49, ст. 6133; № 53, ст. 6554; 2008, № 36, ст. 4087; № 43, ст. 4921; № 47, ст. 5431; 2010, № 17, ст. 2054; № 20, ст. 2435; 2011, № 2, ст. 267; № 9, ст. 1222).